NEWS RELEASE
Marty J. Jackley
South Dakota Attorney General

Charles McGuigan
Chief Deputy Attorney General

FOR IMMEDIATE RELEASE: Tuesday, July 7, 2015
CONTACT: Sara Rabern (605) 773-3215

Attorney General Jackley Calls on Congress to Preserve Authority to Enforce State Data Breach and Data Security Laws

PIERRE, S.D. – Attorney General Marty Jackley and 46 other State and Territorial Attorneys General have asked Congress to recognize the importance of maintaining states' authority to enforce data breach and data security laws, and their ability to enact laws to address future data security risks.

"South Dakota citizens will always be faced with the challenge of monitoring their personal identifying information. States must be able to protect their consumers and respond to these changes in technology and data collection," said Jackley.

The letter points out a number of concerns with federal preemption of state data breach and security laws, including:

- **Data breaches and identity theft continue to cause significant harm to consumers.** Since 2005, nearly 5,000 data breaches have compromised more than 815 million records containing sensitive information about consumers – primarily financial account information, Social Security numbers or medical information. Full-blown identity theft involving the use of a Social Security number can cost a consumer $5,100 on average.

- **Data security vulnerabilities are too common.** States frequently encounter circumstances where data breach incidents result from the failure by data collectors to reasonably protect the sensitive data entrusted to them by consumers, putting consumers' personal information at unnecessary risk. Many of these breaches could have been prevented if the data collector had taken reasonable steps to secure consumers' data.

- **States play an important role responding to data breaches and identity theft.** The States have been at the frontlines in helping consumers deal with the repercussions of a data breach, providing important assistance to consumers who have been impacted by data breaches or who suffer identity theft or fraud as a result, and investigating the causes of data breaches to determine whether the data collector experiencing the breach had reasonable data security in place. Forty-seven states now have laws requiring data collectors to notify consumers when their personal information has been compromised by a data breach, and a number of states have also passed laws requiring companies to adopt reasonable data security practices.

The letter urges Congress to preserve existing protections under state law, ensure that states can continue to enforce breach notification requirements under their own state laws and enact new laws to respond to new data security threats, and to not hinder states that are helping their residents by preempting state data breach and security laws.

-30-